Processing Multilevel Secure Test And Evaluation Information

George Hurlburt
TECNET Executive Secretariat
Naval Air Warfare Center, Aircraft Division

Bradley Hildreth
Concurrent Systems Security Engineering Manager
National Security Agency

Teresa Acevedo
Systems Engineering Manager
Pulse Engineering, Inc.

ITEA 1994 Symposium
"Testing the Global Village"
October 3-6, 1994

Omni Inner Harbor Hotel
Baltimore, MD 21201

Abstract

The Test and Evaluation Community Network (TECNET) is building a Multilevel Secure (MLS) system. This system features simultaneous access to classified and unclassified information and easy access through widely available communications channels. It provides the necessary separation of classification levels, assured through the use of trusted system design techniques, security assessments and evaluations. This system enables cleared T&E users to view and manipulate classified and unclassified information resources either using a single terminal interface or multiple windows in a graphical user interface.

TECNET is in direct partnership with the National Security Agency (NSA) to develop and field the MLS TECNET capability in the near term. The centerpiece of this partnership is a state-of-the-art Concurrent Systems Security Engineering (CSSE) process. In developing the MLS TECNET capability, TECNET and NSA are providing members, with various expertise and diverse backgrounds, to participate in the CSSE process. The CSSE process is founded on the concepts of both Systems Engineering and Concurrent Engineering. Systems Engineering is an interdisciplinary approach to evolve and verify an integrated and life cycle balanced set of system product and process solutions that satisfy customer needs (ASD/ENS-MIL STD 499B 1992). Concurrent Engineering is design and development using the simultaneous, applied talents of a diverse group of people with the appropriate skills. Harnessing diverse talents to support CSSE requires active participation by team members in an environment that both respects and encourages diversity. The synergy of Concurrent Engineering with Systems Engineering results in an explosion of rich design solution sets, maximizing the value-added by TECNET to its users.

To date, the results of the TECNET/NSA partnership are dramatic. The resulting system design meets TECNET growth

expectations, addresses existing national and Department of Defense (DoD) policies, defines the TECNET MLS administrative practices, and is expected to be certified at an acceptable level of risk.

TECNET Background

TECNET exists to support the DoD in the conduct of both developmental and operational Test and Evaluation. This support extends to the United States armed services, defense agencies, the Office of the Secretary of Defense and qualified defense contractors who provide T&E support to the DoD. TECNET offers full featured electronic mail, an extensive bulletin board service, flexible file repository systems for text and binary file exchange, integrated facsimile capabilities, extensive database support, Internet access and specialized information services. TECNET currently serves over 5,500 registered users supporting defense acquisition from the T&E perspective.

Current System Configuration

TECNET operates an accredited C2 level system for unclassified information from the Naval Air Warfare Center - Aircraft Division, Patuxent River, Maryland. This system is accessible via direct dial-up modem lines, the Defense Data Network (DDN), the Defense Research and Engineering Network (DREN), and the Federal Telephone System for the year 2000 (FTS-2000). Another accredited C2 level System High SECRET TECNET capability also operates from the Aberdeen Proving Ground, Aberdeen, Maryland. This system is accessible via the Defense Secure Network 1 (DSNET 1) and via direct dial-up lines utilizing STU-III devices.

It has been a TECNET goal since 1989 to integrate it's classified and unclassified operations. Such integration was perceived as necessary to eliminate the costly redundancy of systems and data brought about by the distinctly separate systems serving the same community. Moreover, user acceptance of the classified capability would be better served if all appropriate data were more accessible in context. For these reasons, TECNET launched a focused applied research and development effort in 1991. This initiative was aimed at better understanding the dynamics and economics of operating an MLS TECNET capability in the not too distant future.

Recent Events

The initial TECNET MLS research, funded through the Defense Acquisition Security Protection (ASP) program, brought TECNET to NSA. A natural union formed as TECNET and NSA learned that many key objectives were mutual and intertwined. As a result of their MLS oriented research program, the TECNET staff became increasingly aware that multiple disciplines would be necessary to field an MLS capability. At the same time, NSA was developing the engineering, management, and documentation concepts underlying an up-front concurrent systems engineering approach. By 1993, the affinity between TECNET's MLS needs and the rapidly maturing NSA CSSE approach became evident. TECNET clearly needed a multi-disciplinary accelerated approach to MLS development at the same time that NSA was constructing a sound CSSE process. A concurrent systems engineering team was formed and working by the end of 1993.

The TECNET team brings several necessary perspectives to the table. The system administration function, system security management role, system engineering activities, network security and planning responsibilities and the program management functions are fully represented within the TECNET team. Additionally, a tri-service certification team is in place to carry out the important, independent task of system certification. These individuals are integrated into the CSSE process. In this and other cases, functional subgroups are identified for separate deliberations in specialty areas, as required. TECNET is also seeking full accreditation through its management structure via the two star Board of Operating Directors (BOOD) for Test and Evaluation. This group oversees the TECNET Steering Committee, which is a multi-service committee responsible for the management of TECNET.

Concurrent Systems Security Engineering Team

The TECNET Executive Secretariat and the NSA CSSE Manager provided the leadership for the MLS TECNET CSSE team. Three primary objectives were identified by the leadership for the CSSE team that served as a focus for the group's efforts and activities. These objectives were used by the team to help drive design alternatives, analysis, and decisions. A set of CSSE principles were developed to govern the dynamics of the CSSE team. The objectives of the CSSE team and the foundation CSSE principles are described below.

Team Objectives

The program plan for MLS TECNET showed an initial operating capability (IOC) of 2nd quarter, Fiscal Year 1995. The highest priority group objective was to perform a certification of the MLS TECNET system and achieve accreditation in time to support the planned IOC. This objective was particularly challenging given the tri-service nature of MLS TECNET. The second objective was to analyze, define, and implement a "system" security solution. In this context, the term "system" is being used to refer to the collection of hardware, software, people, policies, and procedures working together as a whole under regulated conditions. This objective was especially meaningful because the team recognized the potential for the introduction of a

significant administrative burden associated with the use of MLS technology. The third objective was to define a plan for tra ning from the current TECNET system to al of a single MLS host TECNET system supporting access to distributed databases.

Team Principles

In forming the CSSE team, the TECNET leadership established a series of underlying principles that would guide the team's interactions. These principles evolved from the management philosophies of the team leader.

These principles were:

- Each team member must recognize that every team member has value
- Each team member has the same right to attend, speak, and contribute at any team meeting
- Each team member must share in a common goal and know the goal
- Each team member may contribute toward developing the process
- The team must consist of members with the necessary skills (or members having the capability to learn the skills) to achieve the goal
- Each team member must not repeat anything that is said in confidence
- Each team member must be recognized commensurate with their contribution
- Each team member must be prepared to accommodate the learning characteristics (e.g., rates, style) of the other members
- Each team member is expected to maintain an attitude of continual learning.

These principles provided the framework for effective team dynamics. For the CSSE team to achieve its full potential, the team needed a strategy for achieving its goal. This strategy was provided by the CSSE process.

Concurrent Systems Security Engineering Process

The TECNET CSSE team adopted the NSA CSSE process to serve as its roadmap for progress through the development effort. The team was encouraged, by the team leadership, to refine and enhance the process based on the experience of individual members and to tailor the process as necessary for applicability to the MLS TECNET initiative.

Process Description

The CSSE process applied by the CSSE team in the development of MLS TECNET is shown in *Figure 1*. The process shown in *Figure 1* was developed based on the concepts presented in reference papers 1 and 2 (ASD/ENS-MIL STD 499B 1992 and Forsberg and Mooz 1991). The process was refined by the CSSE team to incorporate contributions made by each member. This approach to the CSSE process development encouraged personal commitment to the process from every member of the CSSE team. Additionally, CSSE process definition was enhanced by the diversity of contributions received from area disciplines on the CSSE team.

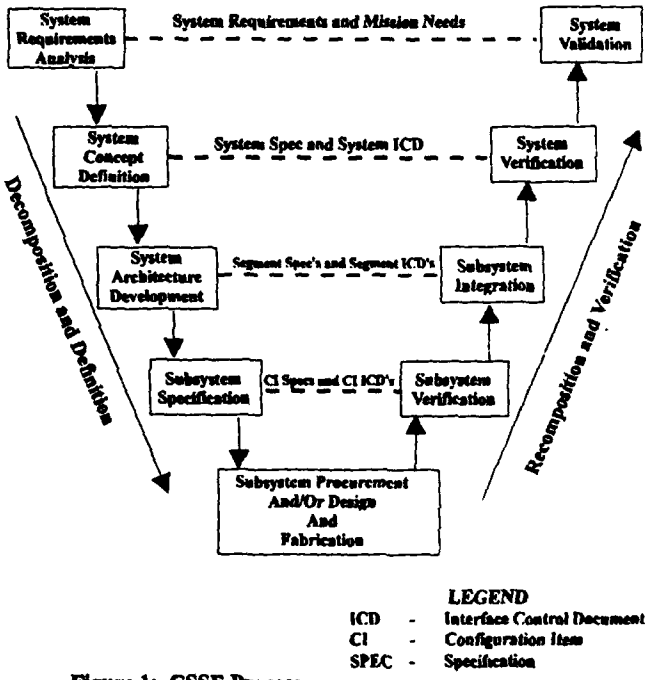

Figure 1: CSSE Process

In *Figure 1*, the leftmost flow from system requirements analysis to subsystem specification represents the system to subsystem decomposition process. At each stage of the development process, the system is further developed and specified in a top down hierarchical fashion. At every level of design decomposition, the 499B model of requirements analysis, functional analysis/allocation, synthesis (physical analysis), and systems analysis and control is applied. At the bottom of this flow the smallest specified units (i.e., subsystems) are either procured or designed and fabricated per the detailed specifications. The rightmost flow from subsystem verification to subsystem validation represents the subsystem to system recomposition process. This rightmost flow indicates that the subsystems are first tested as isolated units against the appropriate subsystem specifications (i.e., verification). The subsystems are then integrated and tested for compliance with system level specifications. Finally, the system is evaluated to determine its effectiveness in meeting customer needs (i.e., validation).

Significant Attributes Of The Process

There are a number of systems engineering process models that have evolved in recent years (e.g., waterfall and spiral). The CSSE team has identified several of the most significant attributes of the CSSE process used by TECNET. These attributes appear to be relevant to any system requiring security regardless of the systems engineering model being applied by the developers.

The significant attributes of the CSSE process are presented below:

- Area disciplines participate in the program from the beginning and are involved throughout the development effort
  - Involvement of policy and doctrine analyst to provide guidance on the policies, laws, and regulations associated with the information processed by the system
  - Involvement of a threat analyst to provide a specific threat profile for the system based on its intended application, the information it processes, and its geographic location
  - Identification and involvement of the Designated Approval Authority, not directly involved in day to day activities, but informed on system objectives and progress
  - Empowerment of the certification officials (TECNET had tri-service issues) to comment on the design during the system engineering process. The certification official is delegated down to a working level to allow a proactive identification of system risk beginning with the requirements analysis through subsystem procurement to system validation
  - Involvement of a security evaluator throughout the design process to provide security design guidance and to participate in the system security risk assessment
  - Involvement of system integrator to provide design guidance that facilitates effective system integration. System integrators additionally are afforded the opportunity to develop a more in depth understanding of system integration requirements by participating in the integration requirements development
  - Involvement of a system administrator to provide design guidance that reduces the potentially significant administrative burden.
- Structured top down design approach
- Identification of design derived requirements for every level of design detail
  - Refinements of initial customer requirements
  - Applicable policy and doctrine
  - Applicable standards
  - Technology constraints
  - Risk assessment and management

- Progressive and structured, informal design reviews
- Subgroups established on an as needed basis with specific objectives for accomplishment and associated timeframes
- Requirements tracking and design compliance analysis for every level of design detail
- Detailed, structured design documentation that can be reused by other similar systems

MLS TECNET is currently in the Subsystem Specification Phase of the CSSE process. While MLS TECNET has not fully executed the CSSE process, the initial results have been extremely encouraging. Each of the CSSE team members have realized value from their involvement in the process.

Benefits To Date

The MLS TECNET effort has realized the following benefits from the CSSE approach:

- Richer design solution set(s) based on diversity and resulting synergy of CSSE team participants
- Customer input and design validation, during the development process, through structured CSSE team meetings
- Up front and concurrent risk identification in a very proactive manner. This enables the team to address security issues early in the process. Early identification of vulnerabilities allows for timely, cost effective, and operationally viable solutions to be proposed
- Documentation of decisions and the rationale behind the decisions facilitates the certification and accreditation effort and provides a focus for additionally required evaluation effort.
- An accelerated integration schedule
- Mutual teaming between agencies that has made the acquisition of funding and skills, such as the certification team, far more credible and easily accomplished
- Mutual respect among the team members that has fostered a professional atmosphere, highly charged with enthusiasm. Such respect could not have emerged without the natural association of TECNET and NSA members.

Conclusions

The activities of the joint TECNET/NSA CSSE team have grown in intensity and significance since the team's inception. The system administration function, system security management role, system engineering activities, network security and planning responsibilities and the program management functions are fully represented within the TECNET team. NSA brings great and complementary expertise to the table. TECNET also has integrated a tri-service certification team into the full CSSE process. The natural dynamic between the operational experience of the TECNET members and the security perspective of the NSA members has produced a meaningful outcome at each stage of the CSSE process. It is this process, which all parties have pledged to follow, that focuses the mutual activities of all concerned. At each stage of this well defined CSSE process the level of specificity grows as the options clearly narrow through strong consensus. While discussion is frequently animated and vivid, the process places clear focus on the ultimate team dynamic. To date, the process has served as the glue that makes the otherwise highly diversified team cohesive.

The benefits of this experience to TECNET have been invaluable. Left to its own devices, TECNET may have reached similar conclusions, but it is doubtful that many of the desirable attributes of the CSSE process would have ever been fulfilled. Moreover, all parties brought skills not easily replicated or even available in each of the complementary organizations (i.e., TECNET and NSA). Finally, joint recognition of the soundness of the CSSE process has helped forge the vital links between the various team players.

Acknowledgements

The authors of this paper would like to thank the members of the MLS TECNET concurrent engineering team for their enthusiasm, contributions, and sincere commitment.

Teresa Acevedo
Pulse Engineering, Inc.
CSSE Consultant

David Ansalvish
Naval Air Warfare Center, Aircraft Division
System Administrator

Lt. Brian Bataille
Headquarters Air Force Systems Operational Test And Evaluation Center
Systems Engineer

Randy Blair
National Security Agency
Risk Assessment Analyst

Rose Benjes
Naval Air Warfare Center, Aircraft Division
TECNET Security Analyst

John Cheng
Pulse Engineering, Inc.
Design Engineer

Stephen Clark
U.S. Army Test and Evaluation Command
Security Chairman

Myron Coplin
Pulse Engineering, Inc.
Design Engineer

Jacquelyn Dinora
Pulse Engineering, Inc.
Documentation Assistant

Dr. Harold Grossman
Clemson University
System Integrator

Mike Harvey
Naval Air Warfare Center, Aircraft Division
Navy Certifier

Bradley Hildreth
National Security Agency
CSSE Manager

Jenny Himes
National Security Agency
Policy and Doctrine Analyst

George Hurlburt
Naval Air Warfare Center, Aircraft Division
TECNET Executive Secretariat

Irene Kempf
National Security Agency
Threat Analyst

Dr. Wayne Madison
Clemson University
System Integrator

Mary Mayonado
Eagan, McAllister Associates, Inc.
TECNET MLS Consultant

John Nicolettos
Pulse Engineering, Inc.
CSSE Consultant

Elizabeth Opp
Naval Air Warfare Center, Aircraft Division
Security Analyst

Shawn Rovansek
Pulse Engineering, Inc.
Design Engineer

Rick Sigman
National Security Agency
Operations Security Analyst

Jim Strom
U.S. Army Chemical, Biological Defense Command
Army Certifier

J. Robert Suckling
U.S. Army Chemical, Biological Defense Command
Army Certifier

Greg Wessel
National Security Agency
Information Systems Security Evaluator

Richard White
Air Force Information Warfare Center
Air Force Certifier

The authors would like to express special thanks to Mr. Charlie Baggett and Mr. Dale Learn for their continuing encouragement and support.

References

- ASD Directorate of Systems Engineering (ASD/ENS) and DSMC Systems Engineering Department (DSMC/FD-SE). May 1992. "Draft Military Standard Systems Engineering (MIL-STD 499B)", 1-54.
- Forsberg, Keven and Mooz, Harold. October 1991. "The Relationship of System Engineering to the Project Cycle." National Council of System Engineering (NCOSE). American Society for Engineering Management (ASEM), 1-11.
- National Computer Security Center. February 1994. "Certification and Accreditation Process Handbook (NCSC-TG-031), 1-140.

ITEA 1994 Symposium
"Testing in the Global Village"
October 3-6, 1994

George Hurlburt
TECNET Executive Secretariat

Naval Air Warfare Center, Aircraft Division

Mr. George F. Hurlburt serves as the newly appointed Technical Director for the Test and Evaluation Corporate Information Management (CIM) initiative within the Joint Program Office for Test and Evaluation (JPO(T&E)). He also serves as the Executive Secretariat for the Test and Evaluation Community Network (TECNET). In this capacity, he works through a designated TECNET deputy. TECNET is responsible to the tri-service TECNET Steering Committee, which in turn, reports to the Board of Operating Directors (BoOD) for Test and Evaluation. Mr. Hurlburt is a senior manager permanently assigned to the Computer Sciences Directorate of the Naval Air Warfare Center - Aircraft Division, Patuxent River, Maryland. Prior to his assignment to TECNET in 1990, he ran the Naval Air Test Center's Information Resources Management (IRM) Office. In this capacity, he successfully launched a Business System Planning (BSP) initiative which led to systematic adoption of corporate information engineering methodologies. Before this assignment, he served as a senior IRM systems analyst responsible for the design and implementation of lasting command wide information systems. Mr. Hurlburt managed the Naval Air Test Center's Technical Information Department and spent eight of his seventeen years at the former Naval Air Test Center as a special assistant on the staff of the Commander.

Mr. Hurlburt is a former Naval Officer and possesses a bachelor of sciences degree from the University of Houston. He is a 1990 graduate of the Naval Air System Command's Senior Executive Management Development Program (SEMDP) and served a one year developmental tour in the Office of the Secretary of Defense.

ITEA 1994 Symposium
"Testing in the Global Village"
October 3-6, 1994

Teresa Acevedo
Systems Engineering Manager

Pulse Engineering, Incorporated

"Ms. Teresa Acevedo is the Manager of Systems Engineering at Pulse Engineering, Inc. She received a Bachelor of Science in Engineering from Loyola College and a Master of Science in Electrical Engineering from Johns Hopkins University. Ms. Acevedo has spent ten years of her professional career in systems engineering, with seven years dedicated to the application of Information Security technology. Ms. Acevedo developed experience in test and evaluation through her work at Westinghouse Electric Corporation, where she was responsible for the testing of the Radar Signal Processor (RSP) of the B-1 Bomber. Ms. Acevedo expanded her systems engineering experience at Booz Allen & Hamilton where she was involved in a variety of systems engineering assignments ranging from Security for the Mexican Election System to the development of a National Electronic Key Management System. More recently, Ms. Acevedo has been responsible for the development of a systems engineering capability at Pulse Engineering. Ms. Acevedo has published several papers on systems engineering that include "Challenges Of Tomorrow - The Future Of Secure Avionics", IEEE 1989 National Aerospace And Electronics Conference, and "Key Management Requirements Of Tactical Air Control Parties (TACP's) In The Tactical Air Control System (TACTS)", AFCEA Security Symposium, August 1990. Ms. Acevedo is a member of the Institue of Electrical and Electronics Engineers (IEEE), Armed Forces Communications Electronics Association (AFCEA), and National Council on Systems Engineering (NCOSE). Ms. Acevedo holds a TOP SECRET SI clearance.

ITEA 1994 Symposium

"Testing in the Global Village"

October 3-6, 1994

Bradley B. Hildreth

Concurrent Systems Security Engineering Manager

National Security Agency

"Mr. Bradley B. Hildreth serves as the Concurrent Systems Security Engineer Manager, providing integrated security services to TECNET within the National Security Agency. He received a Bachelor of Science in Electrical Engineering from Rensselaer Polytechnic Institute and a Master of Science in Applied Behavioral Science from Johns Hopkins University. He is a graduate of the Johns Hopkins Fellowship in Organization and Community Systems. No stranger to the bench, Mr. Hildreth began his career testing integrated circuits. Altogether, he has lived Information Systems Security for the past ten years. His prior assignments have included designing the information protection, access control, and data integrity of a satellite-based data communications system.

He is currently developing the multi-disciplinary information security consulting capability at the National Security Agency. This capability applies the combined efficiencies of Concurrent Engineering, Systems Engineering, Data Capture and Reuse to provide world-class Information Systems Security support - traditionally only available to very large programs - to small and medium sized system development efforts."